Many Bluetooth devices with Google Fast Pair vulnerable to “WhisperPair” hack



Pairing Bluetooth devices can be a pain, but Google Fast Pair makes it almost seamless. Unfortunately, it may also leave your headphones vulnerable to remote hacking. A team of security researchers from Belgium’s KU Leuven University has revealed a vulnerability dubbed WhisperPair that allows an attacker to hijack Fast Pair-enabled devices to spy on the owner.

Fast Pair is widely used, and your device may be vulnerable even if you’ve never used a Google product. The bug affects more than a dozen devices from 10 manufacturers, including Sony, Nothing, JBL, OnePlus, and Google itself. Google has acknowledged the flaw and notified its partners of the danger, but it’s up to these individual companies to create patches for their accessories. A full list of vulnerable devices is available on the project’s website.

The researchers say that it takes only a moment to gain control of a vulnerable Fast Pair device (a median of just 10 seconds) at ranges up to 14 meters. That’s near the limit of the Bluetooth protocol and far enough that the target wouldn’t notice anyone skulking around while they hack headphones.

Once an attacker has forced a connection to a vulnerable audio device, they can perform relatively innocuous actions, such as interrupting the audio stream or playing audio of their choice. However, WhisperPair also allows for location tracking and microphone access. So the attacker can listen in on your conversations and follow you around via the Bluetooth device in your pocket. The researchers have created a helpful video dramatization (below) that shows how WhisperPair can be used to spy on unsuspecting people.

https://arstechnica.com/gadgets/2026/01/researchers-reveal-whisperpair-attack-to-eavesdrop-on-google-fast-pair-headphones/